

CLAIMS

What is claimed is:

- 1 1. A method for control of key pair usage in a computer system, the method
2 comprising:
 - 3 (a) creating key pair material for utilization with an embedded security chip of
4 the computer system, the key pair material including tag data; and
 - 5 (b) determining whether the key pair material is bound to the embedded security
6 chip based on the tag data.
2. The method of claim 1 wherein the tag data further comprises a bit to indicate
whether binding is required for the key pair material.
3. The method of claim 1 wherein creating key pair material further comprises creating
key pair material of different levels.
4. The method of claim 3 wherein the different levels further comprise four levels.
5. The method of claim 4 wherein the four levels further comprise a hardware key pair
level, a platform key pair level, a user key pair level, and a credential key pair level.
6. The method of claim 5 wherein including tag data further comprises including a tag
for indicating binding is required for the platform key pair level.

1 7. A computer system with control over key pair usage, the computer system
2 comprising:
3 a main processor for controlling the computer system; and
4 a security processor coupled to the main processor for embedded security in the
5 computer system, the security processor for storing tag data with key pair material and
6 determining binding of the key pair material to the security processor based on the tag data.

1 8. The system of claim 7 further comprising means for security setup to provide an
2 interface on the computer system for administration of the security processor, including
3 providing the tag data.

1 9. The system of claim 8 wherein the tag data comprises a bit to indicate whether
2 binding is required for the key pair material.

1 10. The system of claim 7 wherein the security processor includes memory for storing
2 the key pair material.

1 11. The system of claim 7 wherein the security processor manages the key pair material
2 in a hierarchical structure.

1 12. The system of claim 11 wherein the hierarchical structure further comprises a four
2 level structure.

1 13. The system of claim 12 wherein the four level structure further comprise a hardware
2 key pair level, a platform key pair level, a user key pair level, and a credential key pair level.

1 14. The system of claim 13 wherein the key pair material further comprises a tag to
2 indicate binding is required for the platform key pair level.

1 15. The system of claim 14 wherein the key pair material further comprises a tag to
2 indicate binding is not required for the user key pair level.

1 16. A method for controlling usage of key pairs in a hierarchical structure of key pairs in
2 an embedded security chip, the method comprising:

3 storing tag data with key pair data for each level of the hierarchical structure; and
4 determining whether the key pair data is bound to the embedded security chip based
5 on the tag data.

1 17. The method of claim 16 wherein storing tag data further comprises storing a set tag
2 bit to indicate that binding is required and storing a reset tag bit to indicate that no binding is
3 required.

1 18. The method of claim 17 further comprising utilizing the reset tag bit with a user key
2 pair level in the hierarchical structure to allow user key pairs to be verified securely on more
3 than one computer system.

